Co-funded by the European Union

Matching of ISO/IEC 27001 and ISO/IEC 27002 as **Lithuanian** standards to **German** “IT-Grundschutz”

ERASMUS+ project "Information Security Awareness, Literacy, and Privacy – ISALIP

Lithuanian Translation of
“Zuordnungstabelle Zuordnung ISO/IEC 27001 sowie ISO/IEC 27002 zum IT-Grundschutz“
(Bundesamt für Sicherheit in der Informationstechnik (BSI) Stand 4. Edition 2021)

This document was produced as part of the ERASMUS+ project "Information Security Awareness, Literacy, and Privacy – ISALIP", Project ID: 2021-2-DE02-KA210-ADU-000051308.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by
the European Union

Paskirstymo lentelė
ISO/IEC 27001 ir ISO/IEC 27002 priskyrimas IT-Grundschutz

"IT-Grundschutz" naudoja BSI 200-1, 200-2 ir 200-3 standartus, kuriuose aprašyta informacijos saugumo valdymo sistemos (ISVS) sukūrimo ir palaikymo procedūra. IT-Grundschutz kompendiume aprašomas susijusių reikalavimų įgyvendinimas. Pagal jį sukurta ISVS atitinka ISO/IEC 27001 reikalavimus ir yra lygiavertė ISO/IEC 27002 rekomendacijoms dėl veiksmų.

Šis palyginimas padeda susieti ISO/IEC 27001:2013 turinį su IT-Grundschutz turiniu. Taip ISO/IEC 27001 aprėptis tampa aiškesnė per pagrindinę IT apsaugą ir palengvinamas papildomos pagrindinės IT apsaugos taikymas taikant ISO standartus.
Šis palyginimas grindžiamas šiomis nagrinėjamų kūrinių versijomis:

- BSI standartas 200-1, 1.0 versija nuo 2017 m. spalio mėn.
- BSI standartas 200-2, 1.0 versija nuo 2017 m. spalio mėn.
- BSI standartas 200-3, 1.0 versija nuo 2017 m. spalio mėn.
- BSI 100-4 standartas, 1.0 versija nuo 2008 m. gruodžio mėn.
- IT-Grundschutz-Kompendium, 4-asis leidimas, 2021 m.
- ISO/IEC 27001:2013 ir ISO/IEC 27002:2013

Jei temos aptariamos viename iš BSI standartų, nurodomas atitinkamo BSI standarto skyrius. Santrumpa (pvz., ISMS.1, ORP.1) nurodo atitinkamą modulį, o "A" - IT-Grundschutz rinkinio reikalavimą. Jei ISO standartų 27001 arba 27002 tema nagrinėjama keliose IT-Grundschutz srityse, pirmiausia susijusi sritis pažymėta **paryškintu šriftu.**

Šio dokumento dalys, susijusios su ISO/IEC 27001 A priedo priemonių tikslais ir priemonėmis bei ISO/IEC 27002 rekomendacijomis, dėl aiškumo atitinka ISO/IEC 27002 struktūrą ir pavadinimus. Išvardytos tik tos ISO/IEC 27002 dalys, kurios susijusios su ISO/IEC 27001 A priedu.

ISO/IEC 27001:2013 ir IT-Grundschutz

		ISO/IEC 27001:2013	IT-Grundschutz
1		Taikymo sritis - taikymo sritis	BSI standartas 200-2, 1 skyrius Įvadas
2		Normatyvinės nuorodos - Normatyvinės nuorodos	BSI standartas 200-1, 11.1 skyrius Bibliografija
3		Terminai ir apibrėžimai - Terminai	BSI kibernetinio saugumo žodynas, https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html
4		**Organizacijos kontekstas - Organizacijos kontekstas**	
	4.1	Organizacijos ir jos konteksto supratimas - Organizacijos ir jos konteksto supratimas	**BSI standartas 200-2, 3.2.1 skyrius Pagrindų sąlygų nustatymas** ISMS.1.A2 Saugumo tikslų ir strategijos nustatymas ORP.5.A1 Pagrindinių sąlygų nustatymas
	4.2	Suinteresuotųjų šalių poreikių ir lūkesčių supratimas - Suinteresuotųjų šalių poreikių ir lūkesčių supratimas	**BSI standartas 200-2, 3.2 skyrius Saugumo proceso projektavimas ir planavimas** **ORP.5.A1 Pagrindinių sąlygų nustatymas**
	4.3	Informacijos saugumo valdymo sistemos apimties nustatymas - Informacijos saugumo valdymo sistemos apimties nustatymas	**BSI 200-2 standarto 3.3.4 skyrius "Apimties nustatymas" ir 8 skyrius "Saugumo koncepcijos sukūrimas pagal standartinį apsaugos metodą".** ISMS.1.A3 Informacijos saugumo gairių sukūrimas
	4.4	Informacijos saugumo valdymo sistema - Informacijos saugumo valdymo sistema	**BSI standartas 200-1, 3 skyrius ISVS apibrėžimas ir proceso aprašymas** **BSI standartas 200-2, 2 skyrius Informacijos saugumo valdymas su IT-Grundschutz** ISMS.1 Saugumo valdymas
5		**Lyderystė - Lyderystė**	
	5.1	Vadovavimas ir įsipareigojimas	**BSI 200-2 standarto 3.1 skyrius Atsakomybės prisiėmimas vadovybės lygmeniu** ISMS.1.A1 Vadovybė prisiima bendrą atsakomybę už informacijos saugumą

		ISO/IEC 27001:2013	IT-Grundschutz
			ISMS.1.A2 Nustatyti saugumo tikslus ir strategiją ISMS.1.A3 Nustatyti informacijos saugumo politiką ISMS.1.A9 Informacijos saugumo integravimas į visos organizacijos procedūras ir procesus
	5.2	Politika - Politika	**BSI standartas 200-2, 3.4 skyrius Informacijos saugumo gairių kūrimas ISMS.1.A3 Informacijos saugumo gairių kūrimas**
	5.3	Organizacijos vaidmenys, pareigos ir įgaliojimai - Organizacijos vaidmenys, pareigos ir įgaliojimai	**BSI standartas 200-2, 4 skyrius Saugumo proceso organizavimas** ISMS.1.A1 Vadovybė prisiima bendrą atsakomybę už informacijos saugumą ISMS.1.A6 Tinkamos informacijos saugumo organizacinės struktūros sukūrimas
6		**Planavimas - Planavimas**	
	6.1	Veiksmai, skirti rizikai ir galimybėms šalinti, - priemonės, skirtos rizikai ir galimybėms šalinti	
	6.1.1	Bendrieji - Bendrieji	**BSI 200-2 standarto 3, 4, 8 ir 9 skyriai**
	6.1.2	Informacijos saugumo rizikos vertinimas - Informacijos saugumo rizikos vertinimas	**BSI 200-2 standarto 3, 4 ir 8 skyriai** BSI standartas 200-3, Rizikos analizė pagal IT-Grundschutz IT-Grundschutz kompendiumo elementarūs pavojai (G0 pavojai)
	6.1.3	Informacijos saugumo rizikos valdymas - Informacijos saugumo rizikos valdymas	**BSI 200-2 standarto 8 ir 9 skyriai** BSI standartas 200-3, Rizikos analizė pagal IT-Grundschutz IT-Grundschutz Compendium
	6.2	Informacijos saugumo tikslai ir jų įgyvendinimo planavimas - Informacijos saugumo tikslai ir jų įgyvendinimo planavimas	**BSI standartas 200-2, 3 skyrius Saugumo proceso inicijavimas**
7		**Parama - pagalba**	
	7.1	Ištekliai - Ištekliai	**BSI 200-1 standarto 5 skyrius Informacijos saugumo ištekliai**

		ISO/IEC 27001:2013	IT-Grundschutz
			ISMS.1.A1 Vadovybė prisiima bendrą atsakomybę už informacijos saugumą ISMS.1.A6 Tinkamos informacijos saugumo organizacinės struktūros sukūrimas ISMS.1.A15 Ekonomiškas informacijos saugumo išteklių naudojimas
	7.2	Kompetencija - Kompetencija	**BSI 200-2 standarto 4.3 skyrius "IS organizacijos užduotys, atsakomybė ir kompetencija".** **ORP.2.A15 Darbuotojų kvalifikacija** ORP.2.A7 Darbuotojų patikimumo tikrinimas
	7.3	Sąmoningumas - Sąmonė	**BSI standartas 200-1, 6 skyrius Darbuotojų įtraukimas į saugumo procesą ORP.3 Informuotumo didinimas ir mokymas apie informacijos saugumą**
	7.4	Komunikacija - Komunikacija	**BSI 200-2 standarto 5.2.4 skyrius Informacijos srautai ir ataskaitų teikimo kanalai**
	7.5	Dokumentais pagrįsta informacija - Dokumentais pagrįsta informacija	
	7.5.1	Bendrieji - Bendrieji	**BSI standartas 200-2, 5 skyrius Dokumentacija saugumo procese** ISMS.1.A13 Saugumo proceso dokumentavimas
	7.5.2	Kūrimas ir atnaujinimas - Kūrimas ir atnaujinimas	**BSI standartas 200-2, 5.2 skyrius Informacijos srautas informacijos saugumo procese** ISMS.1.A13 Saugumo proceso dokumentavimas
	7.5.3	Dokumentuotos informacijos kontrolė - Dokumentuotos informacijos kontrolė	**BSI 200-1 standarto 4.2 skyrius Komunikacija ir žinios** **BSI standartas 200-2, 5.2 skyrius Informacijos srautas informacijos saugumo procese** ISMS.1.A13 Saugumo proceso dokumentavimas
8		**Operacija - Operacija**	

	8.1	Veiklos planavimas ir kontrolė - Veiklos planavimas ir kontrolė	**BSI 200-2 standarto 9 skyrius "Saugumo koncepcijos įgyvendinimas** ISMS.1.A13 Saugumo procesų dokumentacija SYS.1.1.1.A21 Serverio veiklos dokumentacija

		ISO/IEC 27001:2013	IT-Grundschutz
	8.2	Informacijos saugumo rizikos vertinimas - Informacijos saugumo rizikos vertinimas	**BSI 200-2 standarto 3, 4 ir 8 skyriai** BSI standartas 200-3, Rizikos analizė pagal IT-Grundschutz IT-Grundschutz kompendiumo elementarūs pavojai (G0 pavojai)
	8.3	Informacijos saugumo rizikos valdymas - Informacijos saugumo rizikos valdymas	**BSI 200-2 standarto 8 ir 9 skyriai** BSI standartas 200-3, Rizikos analizė pagal IT-Grundschutz IT-Grundschutz Compendium
9		**Veiklos vertinimas - veiklos vertinimas**	
	9.1	Stebėsena, matavimas, analizė ir vertinimas - Stebėsena, matavimas, analizė ir vertinimas	**BSI 200-2 standarto 10 skyrius Informacijos saugumo palaikymas ir nuolatinis gerinimas** ISMS.1.A11 Informacijos saugumo užtikrinimas
	9.2	Vidaus auditas - Vidaus auditas	**BSI 200-2 standarto 10.1 skyrius Informacijos saugumo proceso peržiūra visais lygmenimis** **DER.3.1 Auditai ir peržiūros** **DER.3.2 Pakeitimai pagal IS peržiūros vadovą** ISMS.1.A11 Informacijos saugumo užtikrinimas
	9.3	Valdymo peržiūra - Valdymo vertinimas	**BSI 200-2 standarto 10.1 skyrius Informacijos saugumo proceso peržiūra visais lygmenimis** **BSI 200-2 standarto 10.2 skyrius Informacijos saugumo strategijos tinkamumas** ISMS.1.A11 Informacijos saugumo palaikymas ISMS.1.A12 Informacijos saugumo valdymo ataskaitos
10		**Tobulinimas**	
	10.1	Neatitiktis ir korekciniai veiksmai - Neatitiktis ir korekciniai veiksmai	**BSI 200-2 standarto 10.1 skyrius Informacijos saugumo proceso peržiūra visais lygiais ir 10.3 skyrius Rezultatų pritaikymas informacijos saugumo procese** ISMS.1.A11 Informacijos saugumo užtikrinimas

		ISO/IEC 27001:2013	IT-Grundschutz
	10.2	Nuolatinis tobulinimas	**BSI 200-2 standarto 10 skyrius Informacijos saugumo palaikymas ir nuolatinis gerinimas** ISMS.1.A11 Informacijos saugumo užtikrinimas DER.3.1.1.A1 Atsakomybės apibrėžimas DER.3.2.A9 Integravimas į informacijos saugumo procesą

ISO/IEC 27001:2013 A priedas / ISO/IEC 27002:2013 ir IT-Grundschutz			
		ISO/IEC 27002:2013	**IT-Grundschutz**
5		**Informacijos saugumo politika - Informacijos saugumo gairės**	
	5.1	Informacijos saugumo valdymo gairės - Informacijos saugumo valdymo gairės	
	5.1.1	Informacijos saugumo politika - Informacijos saugumo gairės	**ISMS.1.A3 Informacijos saugumo gairių sukūrimas** BSI standartas 200-2, 3 skyrius Saugumo proceso inicijavimas ISMS.1 Saugumo valdymas ISMS.1.A2 Nustatyti saugumo tikslus ir strategiją ISMS.1.A16 Tikslinėms grupėms skirtų saugumo gairių kūrimas
	5.1.2	Informacijos saugumo politikos apžvalga - Informacijos saugumo politikos apžvalga	**BSI 200-2 standarto 3.4.5 skyrius Saugumo gairių atnaujinimas** ISMS.1 Saugumo valdymas ISMS.1.A11 Informacijos saugumo užtikrinimas
6		**Informacijos saugumo organizavimas - Informacijos saugumo organizavimas**	
	6.1	Vidinė organizacija -Vidinė organizacija	
	6.1.1	Informacijos saugumo vaidmenys ir atsakomybė - Informacijos saugumas	**BSI standartas 200-2, 4.2 skyrius Informacijos saugumo organizacijos struktūra** **ISMS.1.A6 Tinkamos informacijos saugumo organizacinės struktūros sukūrimas**

		Vaidmenys ir atsakomybė	ORP.1.A1 Atsakomybės ir nuostatų nustatymas ORP.1.A2 Atsakomybės paskirstymas ORP.3.A3 Mokyti darbuotojus saugiai naudotis IT OPS.1.1.2.A7 Reglamentuoti IT administravimo veiklą OPS.1.1.3.A2 Apibrėžti atsakomybę DER.3.1.1.A1 Atsakomybės apibrėžimas DER.3.2.A1 Asmenų, atsakingų už IS auditą, paskyrimas IND.1.A1 Integravimas į saugumo organizaciją
	6.1.2	Pareigų atskyrimas - pareigų atskyrimas	**ORP.4.A4 Užduočių paskirstymas ir funkcijų atskyrimas** ORP.1.A4 Nesuderinamų užduočių funkcijų atskyrimas
	6.1.3	Ryšiai su valdžios institucijomis - Ryšiai su valdžios institucijomis	**DER.4 Nepaprastųjų situacijų valdymas** **THE 2.1 Saugumo incidentų nagrinėjimas** **DER.2.1.1.A4 Pranešimas susijusiems subjektams apie saugumo incidentus** DER.2.1.1.A3 Atsakomybės ir kontaktinių asmenų, atsakingų už saugumo incidentus, nustatymas DER.2.1.1.A9 Pranešimo apie saugumo incidentus kanalų nustatymas DER.2.1.1.A14 Saugumo incidentų eskalavimo strategija
	6.1.4	Ryšiai su specialiųjų interesų grupėmis - Ryšiai su specialiųjų interesų grupėmis	**DER.1.A12 Iš išorės šaltinių gautos informacijos vertinimas** ISMS.1.A6 Sukurti tinkamą informacijos saugumo organizacinę struktūrą ISMS.1.A11 Palaikyti informacijos saugumą IND.1.A12 Nustatyti pažeidžiamumo valdymą
	6.1.5	Informacijos saugumas projektų valdyme - Informacijos saugumas projektų valdyme	**ISMS.1 Saugumo valdymas** **ISMS.1.A9 Informacijos saugumo integravimas į visos organizacijos procedūras ir procesus**
	6.2	Mobilieji įrenginiai ir nuotolinis darbas - Mobilieji įrenginiai ir nuotolinis darbas	

	6.2.1	Mobiliųjų įrenginių politika - Mobiliųjų įrenginių politika	**INF.9 Mobilioji darbo vieta** **INF.9.A2 Mobiliųjų darbo vietų taisyklės INF.9.A8** **Mobiliųjų darbo vietų saugos gairės**

			SYS.3.1 Nešiojamieji kompiuteriai SYS.3.2.1 Bendrieji išmanieji telefonai ir planšetiniai kompiuteriai SYS.3.2.2 Mobiliųjų įrenginių valdymas (MDM) SYS.3.2.3 "iOS" (skirta įmonėms) SYS.3.2.4 "Android" SYS.3.3 Mobilusis telefonas SYS.3.1.1.A1 Nešiojamųjų kompiuterių mobiliojo naudojimo tvarka SYS.3.1.1.A14 Tinkamas nešiojamųjų kompiuterių saugojimas SYS.3.2.1.A10 Darbuotojų mobiliųjų įrenginių naudojimo politika SYS.3.2.2.2.A1 Nustatyti mobiliųjų įrenginių valdymo politiką SYS.3.2.2.2.A2 Apibrėžti leidžiamus mobiliuosius įrenginius IND.1.A9 Ribotas išimamųjų laikmenų ir mobiliųjų terminalų naudojimas ICS aplinkoje
	6.2.2	Nuotolinis darbas - nuotolinis darbas	**OPS.1.2.4 Nuotolinis darbas** **OPS.1.2.4.A1 Nuotolinio darbo tvarka**
7		**Žmogiškųjų išteklių saugumas - Personalo saugumas**	
	7.1	Prieš įsidarbinant - Prieš įsidarbinant	
	7.1.1	Atranka - saugos patikrinimas	**ORP.2.A7 Darbuotojų patikimumo patikrinimas ORP.2.A13 Saugumo patikrinimas** ORP.2 Personalas OPS.1.1.1.2.A14 Administratorių patikimumo patikrinimas OPS.1.1.6.A16 Testuotojų patikimumo patikrinimas OPS.2.2.A19 Darbuotojų patikimumo patikrinimas OPS.3.1.A16 Darbuotojų patikimumo patikrinimas

	7.1.2	Įdarbinimo sąlygos -	**ORP.2.A4 Nustatyti išorės darbuotojų samdymo taisykles**

		Įdarbinimo ir sutarčių sąlygos	**ORP.2.A14 Darbuotojų pareigos ir atsakomybė** ORP.2 Personalas ORP.2.A1 Reglamentuotas naujų darbuotojų įvadinis mokymas
	7.2	Įdarbinimo metu - Įdarbinimo metu	
	7.2.1	Vadovybės atsakomybė - Vadovybės atsakomybė	**ISMS.1.A1 Vadovybė prisiima bendrą atsakomybę už informacijos saugumą** ORP.3 Didinti informuotumą ir rengti mokymus apie informacijos saugumą ORP.2.A4 Nustatyti išorės darbuotojų pasitelkimo taisykles ORP.3.A1 Didinti institucijos vadovybės informuotumą apie informacijos saugumą ORP.3.A3 Mokyti darbuotojus saugiai naudotis IT ORP.3.A4 Suplanuoti informuotumo apie informacijos saugumą ir mokymo programą
	7.2.2	Informuotumas, švietimas ir mokymas apie informacijos saugumą - Informuotumas, švietimas ir mokymas apie informacijos saugumą - Informuotumas, švietimas ir mokymas apie informacijos saugumą -mokymai	**ORP.3 Informuotumas apie informacijos saugumą ir mokymas** ORP.3.A1 Didinti institucijos vadovybės informuotumą apie informacijos saugumą ORP.3.A4 Informacijos saugumo mokymo ir informuotumo didinimo programos kūrimas ir planavimas ORP.3.A6 Vykdyti informuotumo apie informacijos saugumą ir mokymus ORP.3.A8 Mokymosi rezultatų matavimas ir vertinimas
	7.2.3	Drausminis procesas	**DER.2.1 Saugumo incidentų nagrinėjimas** **ISMS.1.A8 Darbuotojų įtraukimas į saugumo procesą** ISMS.1.A3 Nustatyti informacijos saugumo politiką ORP.3.A3 Instruuoti darbuotojus apie saugų IT tvarkymą IND.1.A7 Nustatykite išsamų leidimų valdymą tarp OT ir biure. IT

	7.3	Darbo sutarties nutraukimas ir darbo vietos pakeitimas - Darbo sutarties nutraukimas ir darbo vietos pakeitimas	
	7.3.1	Atsakomybė nutraukus arba pakeitus darbo sutartį - Atsakomybė nutraukus arba pakeitus darbo sutartį	**ORP.2.A2 Reglamentuota darbuotojų išvykimo tvarka ORP.4.A2 Įgaliojimų nustatymas, keitimas ir panaikinimas** ORP.2 Personalas ORP.2.A4 Nustatyti išorės darbuotojų samdymo taisykles ORP.4.A1 Naudotojų ir naudotojų grupių kūrimo ir šalinimo taisyklės
8		**Turto valdymas - vertybių valdymas**	
	8.1	Atsakomybė už turtą - Atsakomybė už vertybes	
	8.1.1	Turto inventorizacija - Vertybių inventorizacija	**BSI 200-2 standarto 8.1 skyrius Struktūrinė analizė** **ORP.1.A8 Išteklių ir įrangos valdymas** ISMS.1 Saugumo valdymas ORP.1 Organizacija APP.6.A9 Programinės įrangos inventorizacija IND.1.A4 OT infrastruktūros dokumentacija NET.1.1.1.A2 Tinklo dokumentacija INF.11.A5 Inventorizacijos sąrašo parengimas
	8.1.2	Turto nuosavybė - atsakomybė už vertybes	**ORP.1.A2 Atsakomybės paskirstymas**
	8.1.3	Priimtinas turto naudojimas - Priimtinas vertybių naudojimas	**BSI standartas 200-2, 5.1 skyrius Informacijos klasifikavimas** **ORP.3.A3 Personalo instruktavimas, kaip saugiai tvarkyti IT** ORP.2.A4 Išorės darbuotojų pasitelkimo tvarkos nustatymas CON.9.A4 Keitimosi informacija su išorės šalimis tvarka SYS.3.1.A14 Tinkamas nešiojamųjų kompiuterių saugojimas

			SYS.4.5.5.A5 Išimamosios atminties įrenginio reguliavimas INF.7.A7 Tinkamas oficialių dokumentų ir duomenų laikmenų saugojimas INF.9.A2 Mobiliųjų darbo vietų taisyklės INF.9.A8 Mobiliųjų darbo vietų saugos gairės
	8.1.4	Turto grąža -Vertės grąža	**ORP.2.A2 Reglamentuota darbuotojų išvykimo tvarka ORP.4.A2 Įgaliojimų nustatymas, keitimas ir panaikinimas** ORP.2.A4 Nustatyti išorės darbuotojų pasitelkimo tvarką OPS.2.1.A15 Tvarkingas užsakomųjų paslaugų teikimo santykių nutraukimas OPS.2.2.A14 Tvarkingas debesijos naudojimo santykių nutraukimas
	8.2	Informacijos klasifikavimas - Informacijos klasifikavimas	
	8.2.1	Informacijos klasifikavimas - Informacijos klasifikavimas	**BSI 200-2 standarto 5.1 skyrius Informacijos klasifikavimas BSI 200-2 standarto 8.2 skyrius Apsaugos poreikių nustatymas** ISMS.1 Saugumo valdymas ISMS.1.A10 Saugumo koncepcijos sukūrimas OPS.3.1.1.A3 Užsakomųjų paslaugų projekto saugumo koncepcijos parengimas
	8.2.2	Informacijos ženklinimas - Informacijos ženklinimas	**BSI standartas 200-2, 5.1 skyrius Informacijos klasifikavimas** ISMS.1 Saugumo valdymas
	8.2.3	Turto tvarkymas - Vertybių tvarkymas	**BSI 200-2 standarto 5.1 skyrius Informacijos klasifikavimas BSI 200-2 standarto 8.2 skyrius Apsaugos poreikių nustatymas ISMS.1.A9 Informacijos saugumo integravimas į visos organizacijos procedūras ir procesus** SYS.4.5.5.A13 Tinkamas laikmenų ženklinimas vežant
	8.3	Žiniasklaidos tvarkymas - duomenų laikmenų tvarkymas	

	8.3.1	Kilnojamųjų laikmenų valdymas - Kilnojamųjų laikmenų tvarkymas	**SYS.4.5 Išimamas diskas** **SYS.4.5.5.A4 Nustatykite saugaus kilnojamųjų atminties įrenginių tvarkymo politiką.** SYS.2.1.1.A24 Išorinių ir keičiamųjų laikmenų tvarkymas

			SYS.4.5.5.A1 Didinti darbuotojų informuotumą apie saugų darbą su keičiamosiomis laikmenomis SYS.4.5.A5 Keičiamųjų laikmenų paėmimo reglamentavimas SYS.4.5.A6 Diskų valdymas SYS.4.5.A10 Disko šifravimas
	8.3.2	Laikmenų šalinimas - Duomenų laikmenų šalinimas	**CON.6 Ištrinti ir sunaikinti**
	8.3.3	Fizinės laikmenos perdavimas - duomenų laikmenų gabenimas	**SYS.4.5.5.A14 Saugus siuntimo būdas ir pakuotė** SYS.4.5 Išimamas diskas SYS.4.5.5.A5 Išimamų laikmenų perdavimo politika SYS.4.5.5.A6 Laikmenų valdymas INF.8.A2 Darbinės medžiagos gabenimas į darbo vietą namuose
9		**Prieigos kontrolė - Prieigos kontrolė**	
	9.1	Prieigos kontrolės verslo reikalavimai - Prieigos kontrolės verslo reikalavimai	
	9.1.1	Prieigos kontrolės politika - Prieigos kontrolės politika	**CON.4 Tapatybės ir įgaliojimų valdymas** APP.2.1 Bendroji katalogų tarnyba APP.2.2 "Active Directory APP.2.3 "OpenLDAP ORP.4.A1 Naudotojų ir naudotojų grupių nustatymo ir panaikinimo reglamentas ORP.4.A2 Leidimų nustatymas, keitimas ir panaikinimas ORP.4.A4 Užduočių paskirstymas ir pareigų atskyrimas ORP.4.A5 Prieigos leidimų paskirstymas ORP.4.A6 Prieigos leidimų paskirstymas ORP.4.A7 Prieigos teisių paskirstymas ORP.4.A16 Prieigos ir prieigos kontrolės politika

	9.1.2	Prieiga prie tinklų ir tinklo paslaugų - Prieiga prie tinklų ir tinklo paslaugų	**CON.4 Tapatybės ir įgaliojimų valdymas** APP.2.1 Bendroji katalogų tarnyba APP.2.2 "Active Directory APP.2.3 "OpenLDAP NET.1.1 Tinklo architektūra ir projektavimas NET.1.2 Tinklo valdymas NET.2.1 WLAN veikimas NET.2.2 WLAN naudojimas NET.3.2 Ugniasienė NET.3.3 VPN NET.1.1.1.A4 Tinklų atskyrimas zonose NET.1.1.1.A18 Interneto ryšio P-A-P struktūra NET.1.1.1.A22 Segmentavimo koncepcijos specifikacija NET.1.2.A11 Tinklo valdymo saugumo politikos nustatymas NET.1.2.A13 Tinklo valdymo koncepcijos nustatymas NET.3.1.A24 Tinklo prieigos kontrolės priemonių diegimas NET.3.2.A1 Saugumo politikos kūrimas NET.3.2.A2 Ugniasienės taisyklių nustatymas INF.10.A6 Saugių tinklo prieigų sukūrimas
	9.2	Naudotojo prieigos valdymas - Naudotojo prieigos valdymas	
	9.2.1	Vartotojo registravimas ir išregistravimas - Vartotojo registravimas ir išregistravimas	**ORP.4.A1 Naudotojų ir naudotojų grupių kūrimo ir šalinimo taisyklės** CON.4 Tapatybės ir įgaliojimų valdymas ORP.2.A2 Reglamentuota darbuotojų išvykimo procedūra ORP.4.A2 Įgaliojimų nustatymas, keitimas ir panaikinimas ORP.4.A3 Vartotojo ID ir teisių profilių dokumentavimas ORP.4.A15 Požiūris į tapatybės ir autorizacijos valdymo procesus ir jų kūrimas OPS.1.1.1.2.A4 IT administratoriaus darbo sutarties nutraukimas

	9.2.2	Naudotojo prieigos suteikimas - Priskyrimas	**ORP.4.A16 Prieigos ir prieigos kontrolės politika** ORP.4.A2 Privilegijų nustatymas, keitimas ir panaikinimas

		Naudotojo prieiga	ORP.4.A6 Prieigos teisių suteikimas ORP.4.A7 Prieigos teisių suteikimas
	9.2.3	Privilegijuotų prieigos teisių valdymas - Privilegijuotų prieigos teisių valdymas	**ORP.4.A16 Prieigos ir prieigos kontrolės politika** OPS.1.1.1.2 Tinkamas IT administravimas OPS.1.1.2.2.A4 IT administratoriaus veiklos nutraukimas OPS.1.1.1.2.A5 Administracinės veiklos atsekamumas OPS.1.1.2.A6 Administracinės veiklos apsauga OPS.1.1.2.2.A15 Administracinės veiklos padalijimas OPS.1.1.1.2.A16 Administracinės prieigos apribojimai OPS.1.1.1.2.A17 IT administravimas taikant dvigubos kontrolės principą OPS.1.1.1.2.A18 Nuoseklus administracinės veiklos registravimas APP.2.1.1.A12 Žinyno paslaugų stebėjimas SYS.2.2.2.3.A20 Vartotojo paskyros valdymo UAC naudojimas privilegijuotosioms paskyroms
	9.2.4	slaptos naudotojų autentiškumo patvirtinimo informacijos valdymas - slaptos naudotojų autentiškumo patvirtinimo informacijos valdymas	**ORP.4.A8 Slaptažodžių naudojimo reglamentavimas** ORP.4.A11 Iš naujo nustatyti slaptažodžius ORP.4.A13 Tinkamas autentiškumo patvirtinimo mechanizmų pasirinkimas ORP.4.A23 Slaptažodžių apdorojimo programų ir IT sistemų reglamentavimas
	9.2.5	Naudotojo prieigos teisių peržiūra - Naudotojo prieigos teisių peržiūra	**ORP.4.A3 Vartotojo ID ir teisių profilių dokumentacija** ORP.4.A6 Prieigos teisių suteikimas ORP.4.A7 Prieigos teisių suteikimas
	9.2.6	Prieigos teisių panaikinimas arba patikslinimas - Prieigos teisių panaikinimas arba patikslinimas	**ORP.4.A2 Privilegijų nustatymas, keitimas ir panaikinimas** ORP.2.A2 Reglamentuota darbuotojų išvykimo tvarka ORP.2.A4 Išorės darbuotojų samdymo taisyklių nustatymas ORP.4.A1 Naudotojų ir naudotojų grupių kūrimo ir šalinimo taisyklės ORP.4.A16 Prieigos ir prieigos kontrolės politika

	9.3	Naudotojo pareigos - Naudotojo pareigos	

	9.3.1	Slaptos autentiškumo patvirtinimo informacijos naudojimas - Slaptos autentiškumo patvirtinimo informacijos naudojimas	**ORP.4.A8 Slaptažodžių naudojimo reglamentavimas** **ORP.4.A19 Instruktuokite visus darbuotojus, kaip naudotis autentiškumo patvirtinimo procedūromis ir mechanizmais.**
	9.4	Sistemų ir taikomųjų programų prieigos kontrolė - Sistemų ir taikomųjų programų prieigos kontrolė	
	9.4.1	Informacijos prieigos apribojimas - Informacijos prieigos apribojimas	**ORP.4.A7 Prieigos teisių suteikimas** ORP.4.A1 Naudotojų ir naudotojų grupių kūrimo ir naikinimo taisyklės ORP.4.A16 Prieigos ir prieigos kontrolės gairės NET.1.1.1.A4 Tinklų atskyrimas zonose NET.1.1.1.A22 Segmentavimo koncepcijos specifikacija NET.1.1.A23 Tinklo segmentų atskyrimas NET.1.1.1.A24 Saugus loginis atskyrimas naudojant VLAN
	9.4.2	Saugios prisijungimo procedūros - Saugios prisijungimo procedūros	**ORP.4.A8 Slaptažodžių naudojimo reglamentavimas** **ORP.4.A23 Slaptažodžių apdorojimo programų ir IT sistemų reglamentavimas** ORP.4.A10 Vartotojo ID, turinčių plačias teises, apsauga ORP.4.A12 Sukurti IT sistemų ir taikomųjų programų autentiškumo nustatymo koncepciją ORP.4.A13 Tinkamai parinkti autentiškumo nustatymo mechanizmus ORP.4.A14 Naudotojų atskyrimo IT sistemoje ar taikomojoje programoje veiksmingumo kontrolė ORP.4.A16 Prieigos ir prieigos kontrolės politika CON.7.A5 Ekrano/kodų užrakto naudojimas OPS.1.1.2.A16 Administracinės prieigos apribojimai SYS.2.1.1.A1 Saugus naudotojo autentiškumo patvirtinimas SYS.2.1.1.A37 Daugiafaktorinio autentiškumo patvirtinimo naudojimas SYS.3.2.2.1.A4 Prieigos apsaugos naudojimas

	9.4.3	Slaptažodžių valdymo sistema - Slaptažodžių valdymo sistema	**ORP.4.A8 Slaptažodžių naudojimo reglamentavimas** **ORP.4.A23 Slaptažodžių apdorojimo programų ir IT sistemų reglamentavimas**

			ORP.4.A13 Tinkamas autentiškumo patvirtinimo mechanizmų pasirinkimas
	9.4.4	Privilegijuotų pagalbinių programų naudojimas - Privilegijuotų pagalbinių programų naudojimas	**CON.4 Tapatybės ir įgaliojimų valdymas** ORP.4.A1 Naudotojų ir naudotojų grupių nustatymo ir panaikinimo reglamentas ORP.4.A2 Leidimų nustatymas, keitimas ir panaikinimas SYS.2.3.3.A7 Ribotas teisių priskyrimas rinkmenoms ir katalogams SYS.4.4.A15 Ribojančių teisių priskyrimas
	9.4.5	Prieigos prie programų pirminio kodo kontrolė - Prieigos prie programų pirminio kodo kontrolė	**ORP.4 Tapatybės ir įgaliojimų valdymas CON.8 Programinės įrangos kūrimas CON.8.A10 Šaltinio kodo versijų valdymas** OPS.1.1.1.6.A7 Programinės įrangos testuotojų personalo atranka OPS.1.1.1.6.A13 Bandomosios aplinkos atskyrimas nuo gamybinės aplinkos SYS.2.3.3.A5 Saugus programinės įrangos paketų diegimas SYS.4.4.A15 Ribojančių teisių priskyrimas
10		**Kriptografija - Kriptografija**	
	10.1	Kriptografinė kontrolė - Kriptografinės priemonės	
	10.1.1	Kriptografinių kontrolės priemonių naudojimo politika - Kriptografinių priemonių naudojimo politika	**CON.1 Kriptografijos sąvoka** CON.1.A7 Nustatyti kriptografinių procesų ir produktų naudojimo saugumo politiką CON.1.A10 Sukurti kriptografijos koncepciją
	10.1.2	Raktų valdymas - Raktų valdymas	**CON.1 Kriptografijos sąvoka** CON.1.A1 Tinkamų kriptografinių procedūrų parinkimas CON.1.A2 Duomenų apsauga naudojant kriptografines procedūras CON.1.A4 Tinkamas raktų valdymas CON.1.A5 Saugus kriptografinių raktų ištrynimas ir sunaikinimas CON.1.A9 Tinkamo kriptografinio produkto parinkimas

11		**Fizinis ir aplinkos saugumas - Fizinis ir aplinkos saugumas**	
	11.1	Saugios zonos - Saugios zonos	
	11.1.1	Fizinio saugumo perimetras - Fizinio saugumo perimetras	**INF.1.A23 Saugumo zonų formavimas** INF.1 Bendrasis pastatas INF.2 Duomenų centras ir serverinė INF.1.A26 Vartų sargas arba apsaugos tarnyba INF.1.A27 Apsauga nuo įsilaužimo INF.1.A35 Perimetro apsauga INF.2.A1 Reikalavimų apibrėžtis INF.2.A12 Duomenų centro perimetro apsauga INF.2.A24 Vaizdo stebėjimo sistemų naudojimas
	11.1.2	Fizinė įėjimo kontrolė - Fizinė prieigos kontrolė	**INF.1.A7 Prieigos reguliavimas ir kontrolė INF.2.A6 Prieigos kontrolė** INF.1 Bendrasis pastatas INF.2 Duomenų centras ir serverinė INF.5 Techninės infrastruktūros patalpa ir spinta ORP.1.A3 Išorės asmenų priežiūra arba lydėjimas ORP.4.A5 Prieigos leidimų suteikimas INF.1.A12 Raktų valdymas INF.5.A3 Prieigos reguliavimas ir kontrolė
	11.1.3	Biurų, patalpų ir įrenginių apsauga - Biurų, patalpų ir įrenginių apsauga	**Sluoksnio infrastruktūros blokai,** pvz., INF.7 Biuro darbo vieta INF.1.A9 Pastato naudojimo saugumo koncepcija INF.1.A16 Vengti nuorodų į saugotinas pastatų dalis
	11.1.4	Apsauga nuo išorės ir aplinkos grėsmių.	**Infrastruktūros sluoksnio blokai** INF.1.A3 Priešgaisrinės saugos taisyklių laikymasis

		Apsauga nuo išorės ir aplinkos grėsmių	INF.1.A4 Gaisro aptikimas pastatuose INF.1.A9 Pastato naudojimo saugos koncepcija INF.1.A10 Atitiktis atitinkamiems standartams ir taisyklėms INF.1.A25 Tinkamos vietos parinkimas INF.1.A34 Pavojų aptikimo sistema INF.1.A35 Perimetro apsauga INF.2.A9 Gesinimo arba gaisro prevencijos sistemos naudojimas INF.2.A12 Duomenų centro perimetro apsauga INF.2.A13 Pavojų aptikimo sistemų planavimas ir įrengimas INF.2.A21 Atsarginis kompiuterių centras INF.2.A24 Vaizdo stebėjimo sistemų naudojimas INF.2.A28 Aukštesnio lygio pavojaus aptikimo sistemų naudojimas INF.2.A30 Gaisrų gesinimo ar prevencijos įrenginiai
	11.1.5	Darbas saugiose zonose - Darbas saugiose zonose	**Infrastruktūros sluoksnio blokai** INF.1.A9 Pastato naudojimo saugumo koncepcija INF.1.A23 Saugumo zonų sukūrimas INF.2.A1 Reikalavimų nustatymas
	11.1.6	Pristatymo ir pakrovimo vietos - Pristatymo ir pakrovimo vietos	**INF.1.A7 Prieigos reguliavimas ir kontrolė INF.2.A6 Prieigos kontrolė** ORP.1.A3 Išorės asmenų priežiūra arba lydėjimas ORP.4.A5 Įgaliojimų patekti į teritoriją suteikimas INF.1.A9 Pastato naudojimo saugumo koncepcija INF.1.A23 Saugumo zonų sukūrimas INF.1.A26 Vartų sargas arba apsaugos tarnyba INF.1.A34 Pavojaus signalizacijos sistema INF.1.A35 Perimetro apsauga INF.2.A1 Reikalavimų apibrėžtis INF.2.A12 Duomenų centro perimetro apsauga INF.2.A24 Vaizdo stebėjimo sistemų naudojimas

	11.2	Įranga - prietaisai ir ištekliai	
	11.2.1	Įrangos išdėstymas ir apsauga - Įrangos ir išteklių išdėstymas ir apsauga	**Infrastruktūros sluoksnio blokai** SYS.1.1.1.A1 Tinkamas įrengimas INF.7.A7 Tinkamas oficialių dokumentų ir duomenų laikmenų saugojimas
	11.2.2	Pagalbinės komunalinės paslaugos - Komunalinės paslaugos	**INF.1 Bendrasis pastatas** **INF.2 Duomenų centras ir serverinė** **INF.5 Techninės infrastruktūros patalpa ir spinta INF.12** **Kabeliai** INF.2.A3 Nepertraukiamo maitinimo šaltinio naudojimas INF.2.A4 Avarinis maitinimo šaltinio išjungimas INF.2.A5 Oro temperatūros ir drėgmės palaikymas INF.2.A10 Infrastruktūros tikrinimas ir priežiūra INF.2.A11 Automatinis infrastruktūros stebėjimas INF.2.A14 Atsarginės maitinimo sistemos naudojimas INF.2.A16 Oro kondicionavimas duomenų centre INF.2.A19 Techninės infrastruktūros funkcinių bandymų atlikimas INF.2.A25 Nepertraukiamo maitinimo šaltinių perteklinis projektavimas INF.2.A26 Rezervinių maitinimo šaltinių perteklinis projektavimas INF.5.A9 Maitinimo šaltinis INF.5.A10 Oro temperatūros ir drėgmės atitiktis INF.5.A11 Pavojingų skysčių ir dujų linijų vengimas INF.5.A16 Nepertraukiamo maitinimo šaltinio naudojimas INF.5.A17 Infrastruktūros tikrinimas ir priežiūra INF.5.A24 Vėdinimas ir vėsinimas SYS.1.1.1.A15 Nepertraukiamas ir stabilus elektros energijos tiekimas SYS.2.1.1.A39 Nepertraukiamas ir stabilus elektros energijos tiekimas
	11.2.3	Kabelių saugumas - kabelių saugumas	**INF.12 Laidai** INF.1.A13 Prieigos prie skirstomųjų skydų taisyklės

			INF.2.A23 Tinkamas kabelių išdėstymas duomenų centre INF.12.A2 Kabelių tiesimo planavimas INF.12.A5 Elektros instaliacijos reikalavimų analizė INF.12.A10 Kabelių dokumentacija ir ženklinimas INF.12.A11 Neutrali dokumentacija paskirstymo skyduose INF.12.A15 Kabelių tvirtinimas medžiagomis INF.12.A17 IT kabelių atleidimas iš darbo
	11.2.4	Įrangos priežiūra - Įrangos ir eksploatacinių išteklių priežiūra	**OPS.1.1.1.2.A12 Techninės priežiūros ir remonto darbų tvarka** INF.2.A10 Infrastruktūros tikrinimas ir priežiūra INF.5.A17 Infrastruktūros tikrinimas ir priežiūra INF.11.A2 Priežiūra, tikrinimas ir atnaujinimas
	11.2.5	Turto pašalinimas - Vertės pašalinimas	**INF.9.A2 Mobiliųjų darbo vietų taisyklės** CON.7.A13 Būtinų duomenų ir laikmenų gabenimas SYS.4.5.A5 Išimamųjų laikmenų gabenimo tvarka
	11.2.6	Įrangos ir turto saugumas ne patalpose - Įrangos, išteklių ir turto saugumas ne patalpose	**INF.9 Mobilioji darbo vieta** **INF.8 Namų darbo vieta** **OPS.1.2.4 Nuotolinis darbas** **CON.7 Informacijos saugumas keliaujant užsienyje** SYS.3.1 Nešiojamieji kompiuteriai CON.7.A10 Nešiojamųjų IT sistemų ir laikmenų šifravimas SYS.3.1.A14 Tinkamas nešiojamųjų kompiuterių saugojimas SYS.3.2.1.1.A1 Nustatyti išmaniųjų telefonų ir planšetinių kompiuterių naudojimo politiką INF.8.A2 Darbo medžiagą perkelti į namų darbo vietą INF.9.A1 Tinkamas mobiliosios darbo vietos pasirinkimas ir naudojimas INF.9.A2 Mobiliųjų darbo vietų taisyklės INF.9.A8 Mobiliųjų darbo vietų saugos gairės INF.9.A9 Nešiojamųjų IT sistemų ir duomenų laikmenų šifravimas
	11.2.7	Saugus įrangos šalinimas arba pakartotinis naudojimas - Saugus	**CON.6 Duomenų ištrynimas ir sunaikinimas** CON.6.A1 Informacijos ištrynimo ir sunaikinimo schema

		Įrangos ir išteklių šalinimas arba pakartotinis naudojimas	CON.6.A2 Tinkamas įrangos ir informacijos, kurią reikia apsaugoti, ištrynimas ir sunaikinimas CON.6.A13 Sugadintų skaitmeninių laikmenų sunaikinimas CON.6.A14 Laikmenų naikinimas sustiprintu saugumo lygiu SYS.1.1.A25 Kontroliuojamas serverio eksploatavimo nutraukimas SYS.2.1.A27 Kontroliuojamas kliento eksploatavimo nutraukimas SYS.3.2.2.A22 Nuotolinis terminalų ištrynimas ir eksploatavimo nutraukimas SYS.4.4.A20 Kontroliuojamas daiktų interneto įrenginių eksploatavimo nutraukimas NET.4.1.A11 PBX sistemų ir įrenginių eksploatavimo nutraukimas NET.4.2.A12 Saugus VoIP komponentų eksploatavimo nutraukimas
	11.2.8	Neprižiūrima naudotojo įranga - Neprižiūrima naudotojo įranga	**SYS.2.1.1.A1 Saugus naudotojo autentiškumo nustatymas** ORP.3.A3 Darbuotojų mokymas saugiai naudotis IT ORP.4.A9 Identifikavimas ir autentiškumo patvirtinimas CON.7.A5 Ekrano/kodo užrakto naudojimas CON.7.A11 Apsaugos nuo vagysčių įrenginių naudojimas SYS.3.1.A18 Apsaugos nuo vagysčių įrenginių naudojimas INF.7.A7 Tinkamas oficialių dokumentų ir duomenų laikmenų saugojimas INF.9.A3 Prieiga ir prieigos apsauga
	11.2.9	"Švaraus stalo ir švaraus ekrano" politika - tvarkingos darbo aplinkos ir ekrano užraktų politika	**INF.7.A6 Tvarkinga darbo vieta** SYS.4.1 Spausdintuvai, kopijavimo aparatai ir daugiafunkciniai įrenginiai ORP.4.A9 Identifikavimas ir autentiškumo nustatymas SYS.2.1.A1 Saugus naudotojo autentiškumo nustatymas
12		**Operacijų saugumas - Operacinis saugumas**	
	12.1	Veiklos procedūros ir atsakomybė - Veiklos procedūros ir atsakomybė	

	12.1.1	Dokumentuotos darbo procedūros - Dokumentuotos	**OPS.1.1.1.2.A11 IT administravimo veiklos dokumentavimas OPS.1.1.1.3.A11 Nuolatinis informacijos apdorojimo dokumentavimas**

		Darbo procedūros	OPS.1.1.1.2 Tinkamas IT administravimas OPS.1.2.5 Nuotolinė techninė priežiūra ISMS.1.A13 Saugumo proceso dokumentavimas ORP.1.A1 Atsakomybės ir nuostatų apibrėžimas CON.8.A12 Išsami dokumentacija OPS.1.2.5.A7 Dokumentacija atliekant nuotolinę techninę priežiūrą DER.2.1.1.A16 Saugumo incidentų sprendimo dokumentai SYS.1.1.1.A21 Serverio veiklos dokumentai SYS.2.1.A40 Veiklos dokumentai NET.3.1.A9 Veiklos dokumentai NET.3.2.A14 Veiklos dokumentai NET.4.1.1.A10 PBX konfigūracijos dokumentacija ir peržiūra
	12.1.2	Pokyčių valdymas - pokyčių kontrolė	**OPS.1.1.1.3 Pataisų ir pakeitimų valdymas**
	12.1.3	Pajėgumų valdymas - pajėgumų kontrolė	OPS.1.2.2.2.A12 Archyvinių laikmenų saugojimo išteklių stebėjimas DER.1.1.A6 Nuolatinis registravimo duomenų stebėjimas ir vertinimas SYS.1.1.1.A12 Serverio diegimo planavimas SYS.1.1.1.A23 Sistemos stebėjimas ir serverių stebėjimas SYS.1.5.A17 Virtualios infrastruktūros veikimo būsenos ir konfigūracijos stebėjimas SYS.2.1.A29 Sistemos stebėjimas ir klientų stebėjimas NET.1.1.1.A13 Tinklo planavimas NET.1.2.A25 Tinklo komponentų būklės stebėjimas NET.3.2.A23 Sistemos stebėjimas ir vertinimas
	12.1.4	Kūrimo, testavimo ir veiklos aplinkų atskyrimas - Kūrimo, testavimo ir veiklos aplinkų atskyrimas	**OPS.1.1.1.6.A13 Bandomosios aplinkos atskyrimas nuo gamybinės aplinkos** CON.8 Programinės įrangos kūrimas OPS.1.1.6 Programinės įrangos testavimas ir išleidimas CON.8.A3 Kūrimo aplinkos pasirinkimas CON.8.A7 Programinės įrangos testavimas kūrimo metu CON.8.A11 Programinės įrangos kūrimo politikos nustatymas OPS.1.1.6.A1 Programinės įrangos testavimo planavimas OPS.1.1.1.6.A4 Programinės įrangos išleidimas

			SYS.1.1.1.A30 Viena paslauga vienam serveriui SYS.1.5.A10 Virtualių IT sistemų valdymo procesų įdiegimas SYS.1.7.A33 Bandomųjų ir gamybinių sistemų atskyrimas pagal z/OS NET.1.1.1.A22 Segmentavimo koncepcijos specifikacija
	12.2	Apsauga nuo kenkėjiškų programų	
	12.2.1	Kovos su kenkėjiškomis programomis priemonės - Kovos su kenkėjiškomis programomis priemonės	**OPS.1.1.1.4 Apsauga nuo kenkėjiškų programų** DER.2.1 Saugumo incidentų tvarkymas CON.7.A9 Saugus mobiliųjų duomenų laikmenų tvarkymas DER.1.1.A12 Informacijos iš išorės šaltinių vertinimas APP.1.1.1.A3 Saugus dokumentų iš išorės šaltinių atidarymas SYS.1.1.1.A31 Programų baltųjų sąrašų sudarymas IND.1.A3 Apsauga nuo kenkėjiškų programų IND.2.1.A8 Apsauga nuo kenkėjiškų programų
	12.3	Atsarginė kopija - duomenų apsauga	
	12.3.1	Informacijos atsarginės kopijos - Informacijos apsauga	**CON.3 Duomenų atsarginės kopijos koncepcija** CON.3.A5 Reguliarus atsarginių duomenų kopijų darymas CON.3.A6 Duomenų saugumo koncepcijos parengimas CON.3.A10 Darbuotojų pareiga saugoti duomenis CON.3.A12 Tinkamas atsarginių kopijų laikmenų saugojimas
	12.4	Registravimas ir stebėjimas - Registravimas ir stebėjimas	
	12.4.1	Įvykių registravimas - Įvykių registravimas	**OPS.1.1.1.5 Registravimas** OPS.1.1.1.5.A1 Nustatyti registravimo saugumo politiką OPS.1.1.5.5.A3 Konfigūruoti registravimą sistemos ir tinklo lygiu OPS.1.1.5.5.A6 Sukurti centrinę registravimo infrastruktūrą OPS.1.1.5.5.A9 Pateikti registravimo duomenis analizei

	12.4.2	Žurnalo informacijos apsauga	**ORP.4.A16 Prieigos kontrolės politika OPS.1.1.1.5.A10** **Registravimo duomenų prieigos apsauga OPS.1.1.5.A12** **Registravimo duomenų šifravimas** OPS.1.1.1.5 Registravimas OPS.1.1.1.5.A5 Atitiktis teisinei bazei
	12.4.3	Administratoriaus ir operatoriaus žurnalai - Administratoriaus ir operatoriaus žurnalai	**OPS.1.1.1.5.A10 Prieigos prie registravimo duomenų apsauga** **OPS.1.1.1.2.A18 Nuoseklus administracinės veiklos registravimas** OPS.1.1.1.5 Registravimas OPS.1.1.1.5.A5 Atitiktis teisinei bazei
	12.4.4	Laikrodžių sinchronizavimas - Laikrodžių sinchronizavimas	**OPS.1.1.1.5.A4 IT sistemų laiko sinchronizavimas**
	12.5	Operacinės programinės įrangos kontrolė - Operacinės programinės įrangos kontrolė	
	12.5.1	Programinės įrangos diegimas operacinėse sistemose - Programinės įrangos diegimas operacinėse sistemose	**APP.6 Bendroji programinė įranga** OPS.1.1.6 Programinės įrangos testavimas ir išleidimas APP.7 Individualios programinės įrangos kūrimas OPS.1.1.1.3.A9 Naujos aparatinės įrangos bandymų ir priėmimo procedūros APP.6.A1 Programinės įrangos diegimo planavimas APP.6.A4 Programinės įrangos diegimo ir konfigūravimo taisyklės APP.6.A5 Saugus programinės įrangos diegimas APP.6.A8 Įrengimo failų prieinamumo reglamentas
	12.6	Techninių pažeidžiamumų valdymas - techninių pažeidžiamumų tvarkymas	

	12.6.1	Techninių pažeidžiamumų valdymas - Techninių pažeidžiamumų valdymas	**OPS.1.1.1.3.A16 Reguliari informacijos apie pataisymus ir pažeidžiamumus paieška** **DER.1.1.A12 Iš išorės šaltinių gaunamos informacijos vertinimas** OPS.1.1.1.3 Pataisų ir pakeitimų valdymas IND.1.A12 Nustatyti pažeidžiamumo valdymą

	12.6.2	Programinės įrangos diegimo apribojimai - Programinės įrangos diegimo apribojimai	**OPS.1.1.1.3.A9 Naujos techninės įrangos bandymų ir priėmimo procedūros** OPS.1.1.1.3 Pataisų ir pakeitimų valdymas OPS.1.1.6 Programinės įrangos testavimas ir išleidimas APP.7 Individualios programinės įrangos kūrimas OPS.1.1.6.6.A4 Programinės įrangos išleidimas SYS.2.3.3.A5 Saugus programinės įrangos paketų diegimas
	12.7	Informacinių sistemų audito aspektai - Informacinių sistemų auditas	
	12.7.1	Informacinių sistemų audito kontrolė - Informacinių sistemų audito priemonės	**DER.3.1 Auditai ir peržiūros** **DER.3.2 Pakeitimai pagal IS peržiūros vadovą** ISMS.1.A11 Informacijos saugumo užtikrinimas OPS.2.1.A4 Sutarties su užsakomųjų paslaugų teikėju projektas OPS.2.2.2.A13 Įrodymai, kad debesų kompiuterijos naudojimas užtikrina pakankamą informacijos saugumą
13		**Ryšių saugumas - Ryšių saugumas**	
	13.1	Tinklo saugumo valdymas - Tinklo saugumo valdymas	

	13.1.1	Tinklo kontrolė - Tinklo kontrolės priemonės	**NET.1.1 Tinklo architektūra ir projektavimas NET.1.2 Tinklo valdymas** CON.1 Kriptografijos sąvoka NET.1.1 Maršrutizatoriai ir komutatoriai NET.2.1 WLAN veikimas NET.2.2 WLAN naudojimas NET.3.2 Ugniasienė NET.3.3 VPN ORP.4.A13 Tinkamas autentifikavimo mechanizmų pasirinkimas ORP.4.A16 Prieigos ir prieigos kontrolės politika

			DER.1.1.A6 Nuolatinė registro duomenų stebėsena ir vertinimas NET.1.1.1.A4 Tinklo atskyrimas zonose NET.1.1.1.A7 Saugotinos informacijos užtikrinimas NET.1.1.1.A16 Tinklo architektūros specifikacija NET.1.1.1.A22 Segmentavimo koncepcijos specifikacija NET.1.1.1.A23 Tinklo segmentų atskyrimas NET.1.1.1.A34 Kriptografijos metodų naudojimas tinklo lygmeniu NET.1.2.A7 Pagrindinis įvykių registravimas NET.1.2.A9 Tinklo valdymo ryšio ir prieigos prie tinklo valdymo priemonių užtikrinimas NET.1.2.A11 Tinklo valdymo saugumo politikos nustatymas NET.3.1.A24 Tinklo prieigos kontrolės priemonių naudojimas
	13.1.2	Tinklo paslaugų saugumas - Tinklo paslaugų saugumas	**NET.1.1 Tinklo architektūra ir projektavimas NET.1.2 Tinklo valdymas** CON.1 Kriptografijos sąvoka NET.3.1 Maršrutizatoriai ir komutatoriai NET.3.2 Ugniasienė NET.3.3 VPN ORP.4.A13 Tinkamas autentiškumo patvirtinimo mechanizmų pasirinkimas NET.1.1.1.A34 Kriptografinių metodų naudojimas tinklo lygmeniu NET.3.1.A19 Komutatoriaus prievadų apsauga NET.3.1.A24 Tinklo prieigos kontrolės priemonių naudojimas

	13.1.3	Segregacija tinkluose - Segregacija tinkluose	**NET.1.1 Tinklo architektūra ir projektavimas NET.1.2 Tinklo valdymas** NET.1.1.1.A4 Tinklo skaidymas į zonas NET.1.1.1.A5 Kliento ir serverio segmentavimas NET.1.1.1.A6 Terminalų segmentavimas vidaus tinkle NET.1.1.1.A10 DMZ segmentavimas prieigai iš interneto NET.1.1.A18 P-A-P struktūra interneto ryšiui NET.1.1.1.A19 Infrastruktūros paslaugų atskyrimas

			NET.1.1.1.A21 Valdymo srities atskyrimas NET.1.1.A22 Segmentavimo koncepcijos specifikacija NET.1.1.A23 Tinklo segmentų atskyrimas NET.1.1.A24 Saugus loginis atskyrimas pagal VLAN NET.1.1.1.A32 Fizinis valdymo tinklo segmentų atskyrimas NET.1.1.1.A33 Tinklo mikrosegmentavimas NET.1.1.1.A36 Atskyrimas naudojant VLAN, kai taikomi labai aukšti apsaugos reikalavimai NET.1.2.A32 Fizinis valdymo tinklo atskyrimas NET.1.2.A33 Fizinis valdymo segmentų atskyrimas
	13.2	Informacijos perdavimas - Informacijos perdavimas	
	13.2.1	Informacijos perdavimo politika ir procedūros - Informacijos perdavimo politika ir procedūros	**CON.9.A2 Keitimosi informacija reglamentavimas** CON.1 Kripto sąvoka CON.9 Keitimasis informacija APP.1.2 Interneto naršyklė APP.5.3 Bendroji el. pašto klientė ir serveris SYS.3.2.1 Bendrieji išmanieji telefonai ir planšetiniai kompiuteriai SYS.4.5 Išimamosios laikmenos CON.7.A9 Saugus mobiliųjų duomenų laikmenų tvarkymas CON.9.A4 Dalijimosi informacija su išorės šalimis tvarka CON.9.A5 Likusios informacijos pašalinimas prieš atskleidžiant APP.5.3.A6 Elektroninio pašto saugumo politikos nustatymas SYS.4.1.1.A5 Sukurti naudotojų politiką, skirtą spausdintuvų, kopijavimo aparatų ir Daugiafunkciniai įrenginiai

	13.2.2	Susitarimai dėl informacijos perdavimo - Susitarimai dėl informacijos perdavimo	**CON.9.A4 Susitarimai dėl keitimosi informacija su išorės šalimis** CON.9 Keitimasis informacija CON.7.A9 Saugus mobiliųjų duomenų laikmenų tvarkymas CON.9.A2 Keitimosi informacija reglamentavimas APP.5.3.A6 Elektroninio pašto saugumo politikos nustatymas

	13.2.3	Elektroninių pranešimų siuntimas	**Bendrojo el. pašto klientas ir serveris** CON.9 Keitimasis informacija APP.1.2 Interneto naršyklė APP.1.4 Mobiliosios programos (programėlės) CON.1.A3 Ryšių linijų šifravimas
	13.2.4	Konfidencialumo arba informacijos neatskleidimo susitarimai - Konfidencialumo arba informacijos neatskleidimo susitarimai	**ORP.2.A5 Konfidencialumo susitarimai dėl išorės darbuotojų CON.9.A9 Konfidencialumo susitarimai** ORP.2 Personalas ORP.2.A4 Išorės darbuotojų pasitelkimo taisyklių nustatymas OPS.3.1.A5 Išorės paslaugų teikėjo darbuotojų pasitelkimo taisyklės
14		**Sistemų įsigijimas, kūrimas ir priežiūra - Sistemų įsigijimas, kūrimas ir priežiūra**	
	14.1	Informacinių sistemų saugumo reikalavimai - Informacinių sistemų saugumo reikalavimai	

	14.1.1	Informacijos saugumo reikalavimų analizė ir specifikavimas - Informacijos saugumo reikalavimų analizė ir specifikavimas	**APP.6 Bendroji programinė įranga** **APP.7 Individualios programinės įrangos kūrimas** CON.8 Programinės įrangos kūrimas OPS.1.1.1.6 Programinės įrangos bandymai ir išleidimai OPS.1.1.1.3.A9 Naujos techninės įrangos bandymų ir priėmimo procedūros OPS.1.1.1.6.A4 Programinės įrangos išleidimas APP.6.A2 Parengti programinės įrangos reikalavimų katalogą APP.6.A3 Užtikrinti programinės įrangos įsigijimą APP.6.A14 Sertifikuotos programinės įrangos naudojimas

			SYS.4.4.4.A8 Daiktų interneto įrenginių pirkimo kriterijai
	14.1.2	Taikomųjų programų paslaugų saugumas viešuosiuose tinkluose - Taikomųjų programų paslaugų saugumas viešuosiuose tinkluose	**APP.3.2 Žiniatinklio serveris APP.3.1 Žiniatinklio programos** CON.1 Kriptografijos sąvoka ORP.4.A16 Prieigos kontrolės politika CON.1.A1 Tinkamų kriptografijos metodų parinkimas CON.1.A6 Kriptografijos metodų ir produktų poreikių vertinimas APP.3.1.1.A1 Autentiškumo nustatymas žiniatinklio programose APP.3.2.A2 Žiniatinklio serverio failų apsauga APP.3.2.A5 Autentiškumo nustatymas APP.3.2.A14 Nepriekaištingumo patikros ir apsauga nuo kenkėjiškų programų NET.1.1.1.A4 Tinklo atskyrimas zonose NET.1.1.1.A16 Tinklo architektūros specifikacija
	14.1.3	Taikomųjų paslaugų sandorių apsauga - Taikomųjų paslaugų sandorių apsauga	**CON.1 Kriptografijos sąvoka** NET.3.3 VPN CON.1.A1 Tinkamų kriptografinių procedūrų parinkimas CON.1.A6 Kriptografinių procedūrų ir produktų poreikio vertinimas CON.9.A4 Susitarimai dėl keitimosi informacija su išorės šalimis APP.3.1.A1 Autentiškumo nustatymas žiniatinklio programose
	14.2	Saugumas kūrimo ir palaikymo procesuose - Saugumas kūrimo ir palaikymo procesuose	
	14.2.1	Saugios plėtros politika - Saugios plėtros gairės	**CON.8 Programinės įrangos kūrimas** CON.10 Žiniatinklio programų kūrimas APP.7 Individualios programinės įrangos kūrimas CON.8.A11 Programinės įrangos kūrimo politikos nustatymas APP.1.1.A10 Galutinių vartotojų vykdomas programinės įrangos kūrimo reguliavimas

			APP.3.1.A9 Interneto programų viešieji pirkimai

			APP.4.3.A19 Apsauga nuo kenkėjiškų duomenų bazių skriptų APP.7.A5 Tinkama taikomųjų programų kūrimo kontrolė IND.1.A11 Saugūs viešieji pirkimai ir sistemos kūrimas
	14.2.2	Sistemos pakeitimų kontrolės procedūros - sistemos pakeitimų valdymo procedūros	**OPS.1.1.1.3 Pataisų ir pakeitimų valdymas** CON.8 Programinės įrangos kūrimas CON.8.A10 Šaltinio kodo versijų valdymas CON.10.A12 Esminių pakeitimų tikrinimas OPS.1.1.1.3.A9 Naujos techninės įrangos bandymų ir priėmimo procedūros OPS.1.1.1.3.A11 Nuolatinis informacijos apdorojimo dokumentavimas OPS.1.1.6.A4 Programinės įrangos išleidimas APP.6.A9 Programinės įrangos inventorius IND.1.A4 OT infrastruktūros dokumentacija
	14.2.3	Programų techninė peržiūra pakeitus operacinę platformą - Programų techninė peržiūra pakeitus operacinę platformą	**OPS.1.1.1.3.A11 Nuolatinis informacijos apdorojimo dokumentavimas** APP.7 Individualios programinės įrangos kūrimas OPS.1.1.3 Pataisų ir pakeitimų valdymas OPS.1.1.6 Programinės įrangos testavimas ir patvirtinimas OPS.1.1.1.3.A1 Pataisų ir pakeitimų valdymo koncepcija OPS.1.1.1.3.A9 Naujos techninės įrangos bandymų ir priėmimo procedūros OPS.1.1.1.6.A4 Programinės įrangos išleidimas
	14.2.4	Programinės įrangos paketų keitimo apribojimai - Programinės įrangos paketų keitimo apribojimai	**APP.6 Bendroji programinė įranga** **APP.6.A5 Saugus programinės įrangos diegimas** OPS.1.1.1.6 Programinės įrangos bandymai ir išleidimai OPS.1.1.1.3.A9 Naujos techninės įrangos bandymų ir priėmimo procedūros OPS.1.1.1.6.A4 Programinės įrangos išleidimas APP.6.A4 Programinės įrangos diegimo ir konfigūravimo taisyklės APP.6.A10 Nustatykite programinės įrangos naudojimo saugumo politiką.

	14.2.5	Saugių sistemų inžinerijos principai - analizės, kūrimo ir	**CON.8 Programinės įrangos kūrimas APP.3.1 Žiniatinklio programos** OPS.1.1.1.6 Programinės įrangos bandymai ir išleidimai

		Saugių sistemų priežiūra	CON.8.A5 Saugus sistemos projektavimas CON.8.A12 Išsami dokumentacija CON.8.A22 Saugus programinės įrangos projektavimas CON.10.A11 Žiniatinklio programos architektūra SYS.4.3.A7 Įterptųjų sistemų funkcijų realizavimas aparatine įranga IND.1.A11 Saugus pirkimas ir sistemų kūrimas
	14.2.6	Saugi kūrimo aplinka - Saugi kūrimo aplinka	**CON.8 Programinės įrangos kūrimas** CON.8.A3 Kūrimo aplinkos pasirinkimas CON.8.A14 Kūrėjų grupės mokymas informacijos saugumo klausimais OPS.1.1.6.A13 Bandomosios aplinkos atskyrimas nuo gamybinės aplinkos APP.7.A5 Tinkama taikomosios programos kūrimo kontrolė
	14.2.7	Užsakomoji plėtra	**OPS.2.1 Užsakomosios paslaugos klientams OPS.3.1 Užsakomosios paslaugos paslaugų teikėjams** **APP.7 Individualios programinės įrangos kūrimas** OPS.2.1.1.A1 Nustatyti saugumo reikalavimus užsakomųjų paslaugų projektams OPS.2.1.1.A3 Pasirinkti tinkamą užsakomųjų paslaugų teikėją OPS.2.1.A4 Sudaryti sutartį su užsakomųjų paslaugų teikėju OPS.2.1.A5 Parengti užsakomųjų paslaugų strategiją OPS.2.1.1.A6 Užsakomųjų paslaugų projekto saugumo koncepcijos parengimas OPS.2.1.A11 Planuoti ir užtikrinti informacijos saugumą vykdant užsakomųjų paslaugų operacijas. APP.7.A2 Nustatyti programinės įrangos kūrimo proceso saugumo reikalavimus.
	14.2.8	Sistemos saugumo testavimas - sistemos saugumo testavimas	**OPS.1.1.1.6 Programinės įrangos bandymai ir išleidimai** OPS.1.1.1.6.A5 Atlikti programinės įrangos nefunkcinių reikalavimų testavimą OPS.1.1.1.6.A12 Atlikti regresijos testavimą OPS.1.1.1.6.A14 Įsiskverbimo bandymų atlikimas

	14.2.9	Sistemos priėmimo testavimas - Sistemos priėmimo testas	**OPS.1.1.1.6 Programinės įrangos bandymai ir išleidimai** **OPS.1.1.1.3.A9 Naujos techninės įrangos bandymų ir priėmimo procedūros** OPS.1.1.1.3 Pataisų ir pakeitimų valdymas

			APP.7 Individualios programinės įrangos kūrimas ORP.1.A8 Veiklos išteklių ir įrangos valdymas OPS.1.1.6.A4 Programinės įrangos išleidimas APP.7.A8 Ankstyvas asmens, atsakingo už dalyką, dalyvavimas programinės įrangos bandymuose kūrimo metu
	14.3	Bandymo duomenys - Bandymo duomenys	
	14.3.1	Bandymų duomenų apsauga	**CON.8.A7 Programinės įrangos bandymų atlikimas kūrimo metu OPS.1.1.6.A11 Anoniminių arba pseudoniminių bandymų duomenų naudojimas** CON.8.A14 Kūrėjų grupės mokymas informacijos saugumo klausimais OPS.1.1.6.A1 Programinės įrangos bandymų planavimas OPS.1.1.1.6.A13 Bandomosios aplinkos atskyrimas nuo gamybinės aplinkos
15		**Santykiai su tiekėjais - Santykiai su tiekėjais**	
	15.1	Informacijos saugumas santykiuose su tiekėjais - Informacijos saugumas santykiuose su tiekėjais	
	15.1.1	Informacijos saugumo politika santykiams su tiekėjais - Informacijos saugumo politika santykiams su tiekėjais	**OPS.2.1 Užsakomųjų paslaugų teikimas klientams OPS.2.2 Debesijos naudojimas** **OPS.3.1 Užsakomosios paslaugos paslaugų teikėjams** OPS.1.1.1.2.A12 Techninės priežiūros ir remonto darbų tvarka OPS.2.1.1.A1 Nustatyti saugumo reikalavimus užsakomųjų paslaugų projektams OPS.2.1.1.A5 Nustatyti užsakomųjų paslaugų strategiją OPS.2.2.2.A1 Parengti debesijos naudojimo strategiją OPS.2.2.2.A2 Parengti debesijos naudojimo saugumo politiką OPS.3.1.1.A1 Užsakomųjų paslaugų koncepcijos parengimas

	15.1.2	Tiekėjų susitarimų saugumo klausimų sprendimas - Tiekėjų susitarimų saugumo klausimų sprendimas	**OPS.2.1 Užsakomųjų paslaugų teikimas klientams OPS.2.2 Debesijos naudojimas OPS.3.1 Užsakomosios paslaugos paslaugų teikėjams** ISMS.1.A5 Sutarties projektas skiriant išorės informacijos saugumo pareigūną

			OPS.1.2.5.A19 Trečiųjų šalių atliekama nuotolinė techninė priežiūra OPS.2.1.1.A4 Sutarties su užsakomųjų paslaugų teikėju projektas OPS.2.1.A6 Užsakomųjų paslaugų projekto saugumo koncepcijos parengimas OPS.2.2.A7 Debesijos naudojimo saugumo koncepcijos parengimas OPS.2.2.A9 Sutarties su debesijos paslaugų teikėju parengimas OPS.3.1.1.A2 Sutarčių su užsakomųjų paslaugų klientais rengimas OPS.3.1.1.A7 Užsakomųjų paslaugų teikėjo atliekamas kliento atskyrimo koncepcijos parengimas DER.2.2.A13 Bendrieji susitarimai su išorės paslaugų teikėjais APP.3.2.A10 Tinkamos interneto prieglobos parinkimas SYS.1.8.8.A9 Sandėliavimo sprendimo tiekėjų parinkimas IND.2.4.A2 Eksploatavimas pasibaigus garantijai
	15.1.3	Informacinių ir ryšių technologijų tiekimo grandinė - Informacinių ir ryšių technologijų tiekimo grandinė	**OPS.2.1 Užsakomųjų paslaugų teikimas klientams OPS.2.2 Debesijos naudojimas** **OPS.3.1 Užsakomosios paslaugos paslaugų teikėjams** CON.9.A9 Konfidencialumo susitarimai OPS.1.1.1.2.A12 Techninės priežiūros ir remonto darbų tvarka OPS.1.2.5.A19 Trečiųjų šalių atliekama nuotolinė techninė priežiūra DER.4.A16 Pasirengimo ekstremaliosioms situacijoms ir reagavimo į jas planavimas užsakomiesiems komponentams
	15.2	Tiekėjų paslaugų teikimo valdymas - tiekėjų teikiamų paslaugų kontrolė	

	15.2.1	Tiekėjų paslaugų stebėsena ir peržiūra - Tiekėjų paslaugų stebėsena ir peržiūra	**OPS.2.1.A11 Informacijos saugumo planavimas ir palaikymas vykdant užsakomąsias operacijas** **OPS.2.2.A12 Informacijos saugumo užtikrinimas vykdant nuolatines debesijos operacijas** **OPS.3.1.A10 Informacijos saugumo planavimas ir užtikrinimas vykdant nuolatines užsakomąsias operacijas** OPS.2.1 Užsakomųjų paslaugų teikimas klientams OPS.2.2 Debesijos naudojimas OPS.3.1 Užsakomosios paslaugos paslaugų teikėjams

			DER.3.1 Auditai ir peržiūros OPS.2.2.2.A13 Įrodymai, kad debesų kompiuterijos naudojimas užtikrina pakankamą informacijos saugumą
	15.2.2	Tiekėjų paslaugų pakeitimų valdymas - Tiekėjų paslaugų pakeitimų valdymas	**OPS.2.1 Užsakomųjų paslaugų teikimas klientams OPS.2.2 Debesijos naudojimas** **OPS.3.1 Užsakomosios paslaugos paslaugų teikėjams** OPS.1.1.1.3 Pataisų ir pakeitimų valdymas OPS.1.1.3.3.A5 Pakeitimų prašymų tvarkymas OPS.1.1.1.3.A11 Nuolatinis informacijos apdorojimo dokumentavimas
16		**Informacijos saugumo incidentų valdymas - Informacijos saugumo incidentų tvarkymas**	
	16.1	Informacijos saugumo incidentų ir patobulinimų valdymas - Informacijos saugumo incidentų ir patobulinimų valdymas	
	16.1.1	Atsakomybė ir procedūros - Atsakomybė ir procedūros	**DER.2.1 Saugumo incidentų nagrinėjimas** DER.2.1.1.A2 Saugumo incidentų nagrinėjimo politikos nustatymas DER.2.1.1.A3 Nustatyti atsakomybę ir kontaktus saugumo incidentų atveju DER.2.1.A7 Nustatyti saugumo incidentų nagrinėjimo tvarką

	16.1.2	Pranešimas apie informacijos saugumo įvykius - Pranešimas apie informacijos saugumo įvykius	**DER.2.1 Saugumo incidentų nagrinėjimas** **DER.1 Saugai svarbių įvykių nustatymas** DER.2.2 IT teismo ekspertizės nuostatos DER.1.A1 Saugumo politikos, skirtos su saugumu susijusiems įvykiams aptikti, nustatymas DER.1.A3 Pranešimo apie su saugumu susijusius įvykius kanalų nustatymas DER.1.A4 Darbuotojų informuotumo didinimas DER.2.1.1.A9 Pranešimo apie saugumo incidentus kanalų sukūrimas

	16.1.3	Pranešimas apie informacijos saugumo trūkumus - Pranešimas apie informacijos saugumo trūkumus	**DER.2.1 Saugumo incidentų nagrinėjimas** OPS.1.1.1.3.A16 Reguliari informacijos apie pataisymus ir pažeidžiamumus paieška DER.1.1.A12 Iš išorės šaltinių gaunamos informacijos vertinimas DER.2.1.1.A9 Pranešimo apie saugumo incidentus kanalų sukūrimas IND.1.A12 Nustatyti pažeidžiamumo valdymą
	16.1.4	Informacijos saugumo įvykių vertinimas ir sprendimų dėl jų priėmimas - Informacijos saugumo įvykių vertinimas ir sprendimų dėl jų priėmimas	**DER.1 Saugumo incidentų nustatymas DER.2.1 Saugumo incidentų nagrinėjimas** DER.2.1.1.A1 Saugumo incidento apibrėžtis DER.2.1.1.A11 Saugumo incidentų klasifikacija DER.2.1.1.A19 Saugumo incidentų nagrinėjimo prioritetų nustatymas
	16.1.5	Reagavimas į informacijos saugumo incidentus - Reagavimas į informacijos saugumo incidentus	**DER.2.1 Saugumo incidentų nagrinėjimas** DER.2.2 IT teismo ekspertizės nuostatos DER.2.3 Didelio masto saugumo incidentų šalinimas DER.2.1.1.A4 Pranešimas susijusiems subjektams apie saugumo incidentus DER.2.1.1.A5 Saugumo incidentų sprendimas DER.2.2.2.A11 Įrodymų rinkimo dokumentacija
	16.1.6	Mokymasis iš informacijos saugumo incidentų - Informacijos saugumo incidentų pamokos	**DER.2.1 Saugumo incidentų nagrinėjimas** DER.2.1.1.A17 Tolesni veiksmai po saugumo incidentų DER.2.1.1.A18 Tolesnis procesų tobulinimas remiantis saugumo incidentų išvadomis ir pramonės pokyčiais DER.2.1.A22 Peržiūrėti valdymo sistemos, skirtos spręsti su Saugumo incidentai
	16.1.7	Įrodymų rinkimas - Įrodymų rinkimas	**DER.2.1 Saugumo incidentų valdymas DER.2.2.2 IT kriminalistikos parengtis** DER.2.2.2.A5 Įrodymų rinkimo priemonių IT saugumo incidentų atveju gairių parengimas DER.2.2.2.A9 Išankstinė kriminalistiškai svarbių duomenų atranka DER.2.2.2.A11 Įrodymų rinkimo dokumentacija DER.2.2.2.A14 Įrodymų saugojimo standartinių procedūrų nustatymas

			DER.2.2.2.A15 Atlikti įrodymų rinkimo pratybas NET.1.2.2.A35 Įrodymų rinkimo nustatymai
17		**Verslo tęstinumo valdymo informacijos saugumo aspektai - Verslo tęstinumo valdymo informacijos saugumo aspektai**	
	17.1	Informacijos saugumo tęstinumas - Informacijos saugumo palaikymas	
	17.1.1	Informacijos saugumo tęstinumo planavimas - Informacijos saugumo palaikymo planavimas	**DER.4 Nepaprastųjų situacijų valdymas** BSI standartas 200-2, 3 skyrius Saugumo proceso inicijavimas BSI standartas 100-4, Nepaprastųjų situacijų valdymas DER.2.1 Saugumo incidentų nagrinėjimas
	17.1.2	Informacijos saugumo tęstinumo įgyvendinimas - Informacijos saugumo tęstinumo įgyvendinimas	**DER.4 Nepaprastųjų situacijų valdymas** BSI 100-4 standartas, Nepaprastųjų situacijų valdymas DER.2.1 Saugumo incidentų valdymas
	17.1.3	Informacijos saugumo tęstinumo tikrinimas, peržiūra ir vertinimas - tikrinti ir vertinti informacijos saugumo palaikymą.	**DER.4 Nepaprastųjų situacijų valdymas** BSI 100-4 standartas, ekstremalių situacijų valdymas
	17.2	Atleidimai iš darbo - Atleidimai iš darbo	

	17.2.1	Informacijos apdorojimo priemonių prieinamumas - informacijos apdorojimo priemonių prieinamumas	**INF.2 Duomenų centras ir serverinė** DER.4 Nepaprastųjų situacijų valdymas OPS.1.1.1.2.A19 Atsižvelgimas į didelio prieinamumo reikalavimus

		Paslaugos	OPS.1.1.5.A13 Didelio prieinamumo medienos ruošos infrastruktūra APP.3.2.A15 Atleidimas iš darbo APP.3.3.A13 Kopijavimas tarp svetainių SYS.1.1.1.A28 Prieinamumo didinimas atleidžiant darbuotojus iš darbo SYS.1.2.2.A12 Atleidimas iš darbo ir didelis prieinamumas "Windows Server 2012" SYS.1.5.A20 Didelio prieinamumo architektūrų naudojimas SYS.1.8.A22 Labai prieinamo SAN sprendimo diegimas NET.1.1.A28 Labai prieinami tinklo ir saugumo komponentai NET.1.1.A29 Labai prieinamas tinklo jungčių realizavimas NET.1.1.A30 Apsauga nuo paskirstyto paslaugų atsisakymo NET.1.2.A30 Labai prieinamas valdymo sprendimo realizavimas NET.3.1.A26 Didelis prieinamumas INF.2.A21 Alternatyvus kompiuterių centras INF.2.A25 Atsarginių nepertraukiamo maitinimo šaltinių konstrukcija INF.2.A26 Atsarginių rezervinių maitinimo šaltinių konstrukcija
18		**Atitiktis - Atitiktis**	
	18.1	Teisinių ir sutartinių reikalavimų laikymasis - Teisinių ir sutartinių reikalavimų laikymasis	
	18.1.1	Taikytinų teisės aktų ir sutartinių reikalavimų nustatymas - Taikytinų teisės aktų ir sutartinių reikalavimų nustatymas	**ORP.5 Atitikties valdymas (reikalavimų valdymas)** ORP.5.A1 Sistemos nustatymas ORP.5.A2 Sistemos laikymasis ORP.5.A4 Atitikties valdymo planavimas ir organizavimas ORP.2.A14 Darbuotojų pareigos ir atsakomybė
	18.1.2	Intelektinės nuosavybės teisės - Intelektinės nuosavybės teisės	**ORP.5 Atitikties valdymas (reikalavimų valdymas)** ORP.2.A14 Darbuotojų pareigos ir atsakomybė APP.3.2.A7 Interneto pasiūlymų teisinė sistema

	18.1.3	Įrašų apsauga	**ORP.5 Atitikties valdymas (reikalavimų valdymas)** ORP.3.A3 Mokyti darbuotojus saugiai naudotis IT ISMS.1.A13 Dokumentuoti saugumo procesą.
	18.1.4	Privatumas ir asmenį identifikuojančios informacijos apsauga - Privatumas ir asmenį identifikuojančios informacijos apsauga	**ORP.5 Atitikties valdymas (reikalavimų valdymas)** CON.2 Duomenų apsauga ORP.2.A14 Darbuotojų pareigos ir atsakomybė
	18.1.5	Kriptografinės kontrolės reglamentavimas - Kriptografinių priemonių reglamentavimas	**ORP.5 Atitikties valdymas (reikalavimų valdymas)** CON.1.A8 Veiksnių, darančių įtaką kriptografiniams procesams ir produktams, apžvalga CON.1.A9 Tinkamo kriptografinio produkto parinkimas
	18.2	Informacijos saugumo apžvalgos - Informacijos saugumo apžvalgos	
	18.2.1	Nepriklausoma informacijos saugumo peržiūra - Nepriklausoma informacijos saugumo peržiūra	**ISMS.1.A11 Informacijos saugumo užtikrinimas DER.3.1** **Auditai ir peržiūros** **DER.3.2 Pakeitimai pagal IS peržiūros vadovą** BSI 200-2 standarto 10 skyrius Informacijos saugumo palaikymas ir nuolatinis gerinimas ISMS.1 Saugumo valdymas
	18.2.2	Atitiktis saugumo politikai ir standartams - Atitiktis saugumo politikai ir standartams	**ORP.5 Atitikties valdymas (reikalavimų valdymas)** BSI standartas 200-2, 10.1 skyrius Informacijos saugumo proceso peržiūra visais lygiais ISMS.1.A11 Informacijos saugumo palaikymas
	18.2.3	Techninės atitikties peržiūra - atitikties techninėms specifikacijoms peržiūra	**ISMS.1.A11 Informacijos saugumo užtikrinimas**